
CLAIMS

[Utility model registration claim]
[Claim 1] In the data data encryption equipment which receives the cipher enciphered by the private key cryptosystem, decodes this, and obtains a plaintext The key data table which generates the key data which stored two or more cryptographic key data required in order to decode a cipher, and were specified as the cipher input circuit which receives a cipher by the address, The decryption circuit which decrypts by inputting the cipher output of the key data outputted from a key data table, and said cipher input circuit, and outputs the result as plaintext data, By inputting the plaintext data of a decryption circuit and supervising the redundant bit of the plaintext memorized in the plaintext store circuit which memorizes this, and the plaintext store circuit The judgment result of the plaintext significance judging circuit which judges whether it decoded correctly, and a plaintext significance judging circuit is inputted. Data data encryption equipment characterized by having the key data table address generation circuit which increments the one address and supplies address data to said key data table only when significance is not accepted.
[Claim 2] In the data data encryption equipment which receives the cipher enciphered by the private key cryptosystem, decodes this, and obtains a plaintext The cipher input circuit which receives a cipher, and the cipher store circuit which memorizes the output of a cipher input circuit temporarily, The key data table which generates the key data which stored two or more cryptographic key data required in order to decode a cipher, and were specified by the address, The decryption circuit which the cipher which the key data outputted from a key data table and said cipher store circuit memorized is inputted, decodes a code, and outputs the result as plaintext data, By inputting the plaintext data of a decryption circuit and supervising the redundant bit of the plaintext memorized in the plaintext store circuit which memorizes this, and the plaintext store circuit When the judgment result of the plaintext significance judging circuit which judges whether decode was performed correctly, and a plaintext significance judging circuit is inputted and significance is not accepted Data data encryption equipment characterized by having the key data table address generation circuit which continues an increment until it repeats the actuation which increments the one address and supplies address data to said key data table and the judgment result of said plaintext significance judging circuit shows significance.

[Translation done.]

DETAILED DESCRIPTION

[Detailed explanation of a design]
[0001]
[Industrial Application]
This design is related with the decryptor in the cryptocommunication system which used two or more key data.
[0002]
[Description of the Prior Art]
In the field of digital communication, the signal from the information source is changed into the numerical train which generally consists of binary [of "1" and "0"], by modulating a carrier signal with binary [this], is sent out to wireless or a cable-transmission way, and is transmitted to the destination. As a signal from the information source, there are an alphabetic character, voice, an image, etc., for example, and these information source signals are in the situation which a third party can monitor easily on a transmission line. When using the transmission line which a third party can monitor as mentioned above and transmitting information, about the information source data which have secrecy nature, it enciphers by the information source side, and the so-called cryptocommunication system which restores the signal from the information source of even if it decrypts this by the receiving side of the destination is constituted.
[0003]
Although the thing based on various principles is proposed and used as a cryptocommunication system, there are some which are called a private key cryptosystem to one of the methods used well. In the private key cryptosystem, the substitution type which transposes information which replaces the sequence of information, such as an alphabetic character, such as a transposition type and an alphabetic character, to other alphabetic characters etc. is used. The third party who does not know under what kind of regulation information was processed cannot decode the information from the information source which is processed and is sent out to a transmission line by these actuation, but it makes decode possible only by the receiving side of the destination which knows the regulation. Therefore, in the above-mentioned private key cryptosystem, it becomes important to protect the conversion table of substitution, the regulation, i.e., the transposition, used since [to encipher] the transmitting side and the receiving side know, so that it may not be known by the third party. From the conversion table of transposition or substitution being called a key, the above-mentioned method is called a private key cryptosystem. Here, although a fixed period and the same thing are used, in order to secure communicative secrecy nature, it is not desirable [key data] to use the same key data for a long time. It is because sufficient time amount and sufficient opportunities, such as the so-called known plaintext attack, to collect sufficient samples of correspondence with the same key, analyze this, and discover a cryptographic key for a wire-tapping person will be given when a communication link is continued over a long period of time using the same key data. Since discovery of key data becomes still easier when especially the algorithm of a code is exhibited, key data need to be frequently exchangeable.
[0004]
Now, if a transmitting side and a receiving side synchronize and naturally do not exchange in case key data are exchanged, it cannot be overemphasized that a cipher is undecipherable by the receiving side. Then, although delivery of key data is made by various approaches, safety is high if it can deliver for example, with a means different from the channel which sends and receives a cipher. In the system in which the communication link of a cipher is performed by the electrical communication by the cable, considering the case where deliver the time which exchanges cryptographic key data from a transmitting side beforehand, and new cryptographic key data to a receiving side with a physical means, and each parameter of a decryption machine is set based on these by the receiving side, a third party does not have a means to monitor this, but can secure high safety.
[0005]
However, when especially the distance of a transmitting side and a receiving side is remarkably separated and does not have delivery means other than a communicative transmission line (i.e., when it does not have a physical means to deliver key data), the delivery of key data itself will not obtain ******** to the channel which a third party can monitor. In this case, wire tapping whose channel itself which delivers key data is a third party is possible, since there is risk of key data being decoded, renewal of key data will not be performed, but the key data initialized in the key data store circuit will be used continuously. Therefore, the need for a means to exchange key data at insurance in such a case arises.
[0006]
the example of the conventional data data encryption equipment with which drawing 4 possesses the key delivery

means in a private key cryptosystem -- it is -- drawing -- setting -- 1 -- an input cipher and 2 -- a cipher input circuit and 3 -- a cipher and 5 -- key data and 6 -- for a plaintext output circuit and 9, as for a key data distinction circuit and 21, an output plaintext and 20 are [a decryption circuit and 7 / a plaintext and 8 / updating key data and 22] key data store circuits.

[0007]

Next, actuation is explained. It is received in the cipher input circuit 2, and the input cipher 1 is inputted into the decryption circuit 6 as a cipher 3. On the other hand, the key data 5 for decoding a code in the decryption circuit 6 are supplied to the decryption circuit 6 from the key data store circuit 22. Using the key data 5, the decryption circuit 6 decodes a cipher 3 and outputs the result as a plaintext 7. A plaintext 7 is outputted as an output plaintext 9 from the plaintext output circuit 8. The cipher input circuit 2 has the function of the buffer for processing input data in a decryption circuit here. For example, when the input cipher 1 is a serial data format, the cipher input circuit 2 is changed into the parallel data which consist of the number of bits to which the cipher decode circuit 6 processes this simultaneously. Moreover, in the plaintext output circuit 8, it has the function to change again into serial data the parallel data outputted to reverse from a cipher decode circuit.

[0008]

Here, although a cipher 3 is decoded by the decryption circuit 4 and a plaintext 7 is outputted as an output plaintext through the plaintext output circuit 8, a plaintext 7 is simultaneously supplied also to the key data distinction circuit 20. In a key data distinction circuit, if the specific information included in a plaintext 7 is detected and it distinguishes that it is delivery of key data, the detected updating key data 21 will be supplied to the key data store circuit 22. The key data of a key data store circuit are carried out in this way, and are updated, and data with the new key data to the decryption circuit 4 after this are used. In a transmitting side, since it enciphers by updating one's encryption key after delivering the above-mentioned key data, renewal of the key data which synchronized by transmission and the receiving side is attained. When the transmitting side was arbitration, key data are changed, transmit key data from the channel of a cipher as a cipher by the specific approach, this is received in a receiving side, it distinguishes whether it is key data enciphered by the above-mentioned specific approach and it is detected that it is delivery of key data, key data are updated and decryption after this can be carried out with new key data.

[0009]

[Problem(s) to be Solved by the Device]

Also in the communication system which cannot perform delivery of key data through the channel of a cipher, and cannot deliver key data in the aforementioned example other than a cipher channel Although decode of the cryptographic key data by the third party who monitors the above-mentioned channel by delivering key data to arbitration via a cipher channel is difficult On the other hand, when the updating key data once received by the receiving side in the transmitting side according to a certain cause were missed, it did not have a means by which it could be known but the technical problem that the communication link after this became impossible occurred. That is, when the key data written in a key data store circuit contain the error, there is possibility of an error — some bits of the once written-in key data are reversed with a noise or a soft error — of being generated.

[0010]

This design is in the system which cannot but use the transmission line of the communication link by delivery of key data itself to obtain the data data encryption equipment which a third party cannot decode.

[0011]

Future communication links are enabled by detecting that changed into arbitration the key data used by the transmitting side, and key data were changed by the receiving side, and performing subsequent decode using new key data, without delivering from a transmitting side via a communicative transmission line to a receiving side, in order to cope with the conventional technical problem carried out in the first half.

[0012]

[Means for Solving the Problem]

The table which contained two or more key data beforehand is held by the receiving side, a receiving side searches the content of the key data receipt table automatically, without transmitting the key data used from a transmitting side for decryption to a receiving side, and the data data encryption equipment concerning this design makes it possible to decode key data according to the thing of a transmitting side.

[0013]

[Function]

A receiving side detects modification of the key data of a transmitting side automatically, and the data data encryption equipment in this design enables subsequent communication links, also when the key data used by the transmitting side are changed into arbitration.

[0014]

[Example]

Example 1

the block diagram of the data data encryption equipment which drawing 1 shows one example of this design -- it is -- drawing -- setting -- 1 -- an input cipher and 2 -- a cipher input circuit and 3 -- a cipher and 4 -- a key data table and 5 -- for a plaintext and 8, as for an output plaintext and 10, a plaintext output circuit and 9 are [key data and 6 / a decryption circuit and 7 / a plaintext store circuit and 11] storage plaintexts. Moreover, as for the significance judging result flag of a plaintext, and 16, the plaintext significance judging circuit where 12 judges the significance about the storage plaintext 11, the significance level-setting circuit which sets up the level 13 judges

the existence of significance to be, the significance level to which 14 was set, and 15 are [a key data table address generation circuit and 17] the key data table addresses.
[0015]
Now, in the above-mentioned example, the output plaintext 9 of the plaintext output circuit 8 is once memorized in the plaintext store circuit 10, and the storage plaintext 11 of the plaintext store circuit 10 is inputted into the plaintext significance judging circuit 12. In the plaintext significance judging circuit 12, the significance of the storage plaintext 11 is judged on the basis of the significance level 14 beforehand set as the significance level-setting circuit 13, and the result is outputted as a significance judging result flag 15. The key data table address generation circuit 16 does not change the address already set up when it is shown that significance has the above-mentioned significance judging result flag 15, but when it is shown that there is no significance on the other hand, it changes the key data table address 17, and the new data of the key data table 4 are urged to it.
[0016]
The concrete actuation in the above-mentioned example is explained. The key data of N kind (N N>=2 integer) shall be stored in the key data table 4. Suppose that it is also the encryption equipment of a transmitting side in the condition that are completely using the same key data table and the transmitting side and the receiving side are using the n-th key data (n 1 <=n<=N integer) among those now. In this condition, in order to decrypt a receiving side by the transmitting side using the completely same key data as the key data used for encryption, a right plaintext output is obtained. At a certain event, the case where a transmitting side changes key data is considered. When the key data newly chosen by the transmitting side are the thing of eye watch (n+1) of a key data table, a right plaintext output is not obtained as a result decoded by the receiving side using the n-th key data.
At this time, the mistaken output plaintext 9 is memorized in the plaintext store circuit 10, and the significance judging result flag 15 is set to non-significant condition as a result of having judged that significance in the plaintext significance judging circuit 12. In the key data table address selection circuit 16, when a significance judging result flag is non-significant condition, the key data table address 17 is incremented one time. Consequently, the key data which the key data table 4 generates are updated.
[0017]
Example 2
Here, the method of performing the significance judging of a plaintext can consider various kinds of things. For example, a simple example is shown in drawing 2 . In drawing, the 8-bit redundant bit for error detection is added to a 56-bit information bit as a plaintext before being enciphered, and the block cipher which makes a 64-bit plaintext 1 block is considered. A cryptographic key is 64 bits as well as plaintext length, and in a transmitting side, it enciphers according to the algorithm to which the 64-bit cipher was beforehand set with 64-bit key data, and it generates a 64-bit cipher. On the other hand, by the receiving side, this is decrypted with 64-bit key data, and a 64-bit plaintext is reproduced. When the code used by the transmitting side is changed now, by the receiving side, this cannot be known, and in order to decode by different key data from the key data used for encryption, the plaintext data which were mistaken as plaintext data outputted are obtained. Therefore, an error is generated in the 8-bit redundant bit for error detection, and modification of key data can be known by supervising the redundant bit for error detection in the plaintext significance judging circuit 12. Here, the allowance error number of bits is set up in the significance level-setting circuit 13. That is, in not permitting an error at all and permitting 0 bit and an error, it sets up the allowance number of bits beforehand.
[0018]
If an error is detected by key data, the key data table address generation circuit 16 will increment the key data table address 17 one time with the significance judging result flag 15 as mentioned above. In order that the key data table 4 may choose the new key data by which the increment was carried out and may supply them to the decryption circuit 6, decryption after this will be performed using new key data.
[0019]
The key data changed by the transmitting side cannot decode the input cipher after this correctly in the receiving side which incremented one time as mentioned above, when it is not necessarily limited to the next key data table address in use, therefore changes into the key data of for example, 5 address point. In this case, in a transmitting side, if the same new cipher is transmitted 5 times, since a total of five increments of addresses will be carried out by the 5th reception, right decode is attained. In a transmitting side, when key data are changed, it becomes possible to set up the key data of a receiving side correctly by [which incremented at the time of the transmission just behind that] overlapping by the address and transmitting the same cipher.
[0020]
Example 3
Another example of this design is shown in drawing 3 . In drawing, although 1-17 are the same as that of drawing 1 , 18 is a cipher store circuit, it is inserted between the cipher input circuit 1 and the decryption circuit 6, and the storage cipher 19 memorized in the cipher store circuit 18 is supplied to the cipher decode circuit 6. When modification of key data is detected [in / an input cipher is held until the following cipher is inputted, and / the plaintext significance judging circuit 12] by doing in this way, by repeating the increment actuation by the key data table address generation circuit 16, a loop formation is operated continuously and it becomes possible to decode the cipher itself memorized in the cipher store circuit 18. Therefore, updating to decode and new key data is attained, without transmitting the same cipher repeatedly by the transmitting side like an example 1 in this case.
[0021]

[Effect of the Device]
As mentioned above, modification of key data is attained, without delivering key data from a transmitting side to a receiving side in a system without a means to deliver key data in addition to the channel used for transmission and reception of a cipher according to this design. Therefore, also in the communication system which cannot deliver key data other than a cipher channel, it is effective in avoiding the danger of wire tapping considered when delivering key data via a cipher channel, and being able to avoid blocking of the communication link brought about when an error is moreover produced to key data during delivery of key data.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing one example of this design.
[Drawing 2] It is drawing showing actuation of the significance judging circuit of the plaintext used for the data data encryption equipment of this design.
[Drawing 3] It is drawing showing the example of the data data encryption equipment which is one more of the design of this.
[Drawing 4] It is the block diagram of conventional data data encryption equipment.
[Description of Notations]
1 Input Cipher
2 Cipher Input Circuit
3 Cipher
4 Key Data Table
5 Key Data
6 Decryption Circuit
7 Plaintext
8 Plaintext Output Circuit
9 Output Plaintext
10 Plaintext Store Circuit
11 Storage Plaintext
12 Plaintext Significance Judging Circuit
13 Significance Level-Setting Circuit
14 Significance Level
15 Significance Judging Result Flag
16 Key Data Table Address Generation Circuit
17 Key Data Table Address
18 Cipher Store Circuit
19 Storage Cipher
20 Key Data Distinction Circuit
21 Updating Key Data
22 Key Data Store Circuit

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開実用新案公報**（Ｕ）　(11)実用新案出願公開番号

実開平5－63142

(43)公開日　平成５年(1993)８月20日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ　9/06				
9/14				
Ｇ０９Ｃ　1/00		9194－5L		
		7117－5K	Ｈ０４Ｌ　9/ 02	Ｚ

審査請求　未請求　請求項の数２(全　３　頁)

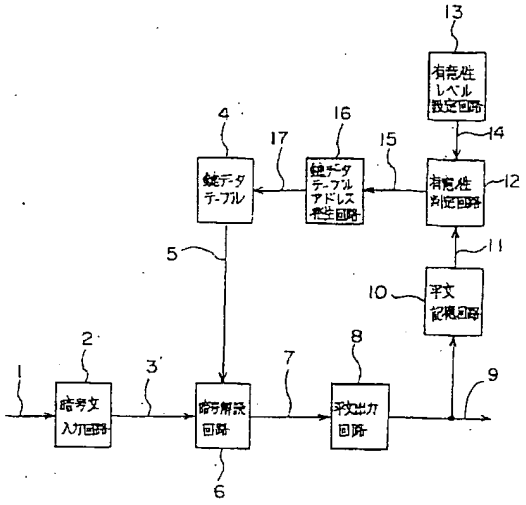
(21)出願番号　実願平4－2892

(22)出願日　平成４年(1992)１月30日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)考案者　三奈木　正純
鎌倉市上町屋325番地　三菱電機株式会社
鎌倉製作所内
(74)代理人　弁理士　高田　守

(54)【考案の名称】　データ暗号装置

(57)【要約】
【目的】　秘密鍵暗号通信系において、送信側と受信側が例えば長い距離で隔てられ、鍵データの配送を、第三者の傍受する通信路を経由する以外に手段のない場合に、鍵データを送信側から受信側に送信することなく、受信側で自動的に新しい鍵データを検索することにより、通信の途絶を回避することが可能なデータ暗号装置を得る。
【構成】　受信側のデータ暗号装置において、あらかじめ複数のデータ鍵を格納した鍵データテーブルを備え、解読後の平文データに含まれる冗長ビットを監視することにより、送信側と異なる鍵データにより解読したことを知り、正しい鍵データテーブルを検索するようにした。



1

〔実用新案登録請求の範囲〕

【請求項1】　秘密鍵暗号方式により暗号化された暗号文を受信し、これを解読して平文を得るデータ暗号装置において、暗号文を受信する暗号文入力回路と、暗号文を解読する為に必要な暗号鍵データを複数格納し、アドレスにより指定された鍵データを発生する鍵データテーブルと、鍵データテーブルから出力される鍵データ及び前記暗号文入力回路の暗号文出力を入力されて暗号解読を行い、その結果を平文データとして出力する暗号解読回路と、暗号解読回路の平文データを入力されて、これを記憶する平文記憶回路と、平文記憶回路に記憶された平文の冗長ビットを監視することによって、解読を正しく行われたか判定を行う平文有意性判定回路と、平文有意性判定回路の判定結果を入力されて、有意性が認められない場合にのみ、アドレスを1つインクリメントして前記鍵データテーブルにアドレスデータを供給する鍵データテーブルアドレス発生回路を備えたことを特徴とするデータ暗号装置。

【請求項2】　秘密鍵暗号方式により暗号化された暗号文を受信し、これを解読して平文を得るデータ暗号装置において、暗号文を受信する暗号文入力回路と、暗号文入力回路の出力を一時的に記憶する暗号文記憶回路と、暗号文を解読する為に必要な暗号鍵データを複数格納し、アドレスにより指定された鍵データを発生する鍵データテーブルと、鍵データテーブルから出力される鍵データ及び前記暗号文記憶回路の記憶した暗号文を入力されて暗号の解読を行い、その結果を平文データとして出力する暗号解読回路と、暗号解読回路の平文データを入力されて、これを記憶する平文記憶回路と、平文記憶回路に記憶された平文の冗長ビットを監視することによって、解読が正しく行われたか判定を行う平文有意性判定回路と、平文有意性判定回路の判定結果を入力されて、有意性が認められない場合には、アドレスを1つインクリメントして前記鍵データテーブルにアドレスデータを＊

2

＊供給する動作を繰り返し、前記平文有意性判定回路の判定結果が有意性を示すまでインクリメントを続ける鍵データテーブルアドレス発生回路を備えたことを特徴とするデータ暗号装置。

【図面の簡単な説明】

【図1】この考案の1実施例を示す構成図である。

【図2】この考案のデータ暗号装置に用いられる平文の有意性判定回路の動作を示す図である。

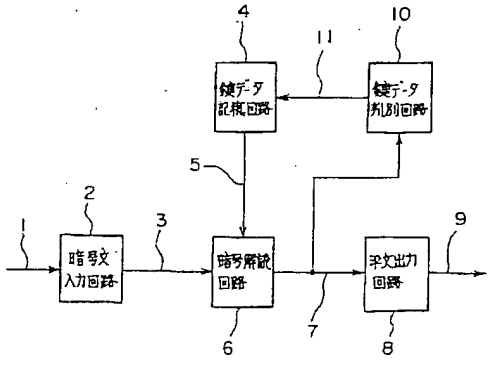
【図3】この考案のもう1つであるデータ暗号装置の実施例を示す図である。

【図4】従来のデータ暗号装置の構成図である。

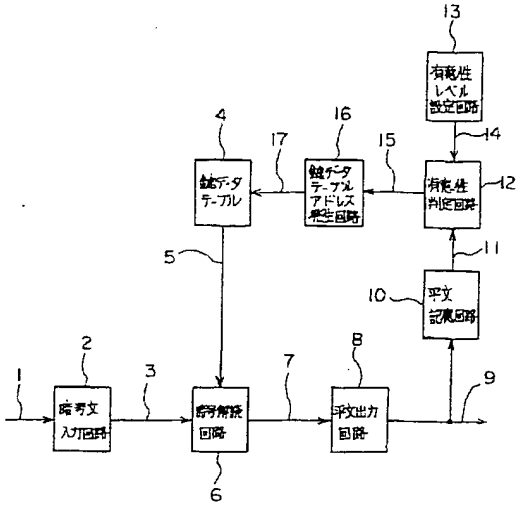
【符号の説明】

1　入力暗号文
2　暗号文入力回路
3　暗号文
4　鍵データテーブル
5　鍵データ
6　暗号解読回路
7　平文
8　平文出力回路
9　出力平文
10　平文記憶回路
11　記憶平文
12　平文有意性判定回路
13　有意性レベル設定回路
14　有意性レベル
15　有意性判定結果フラグ
16　鍵データテーブルアドレス発生回路
17　鍵データテーブルアドレス
18　暗号文記憶回路
19　記憶暗号文
20　鍵データ判別回路
21　更新鍵データ
22　鍵データ記憶回路

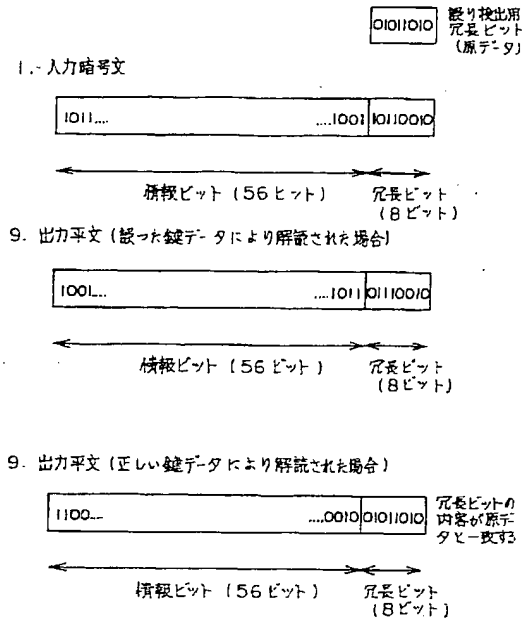
【図4】



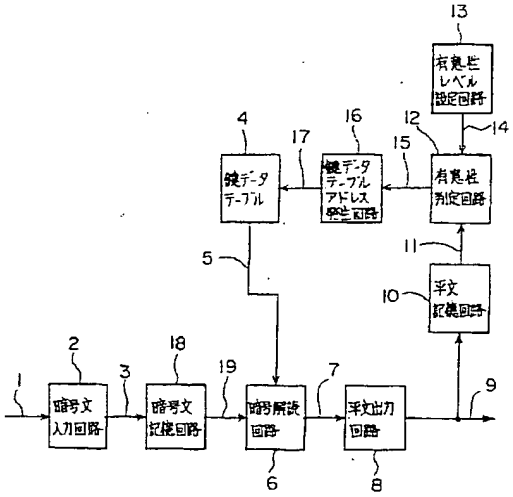
【図1】


13
有意性レベル設定回路
4
16
17
15
14
鍵データテーブル
鍵データテーブルアドレス発生回路
有意性判定回路
12
5
11
10
平文記憶回路
2
8
1
3
7
9
暗号文入力回路
暗号解読回路
平文出力回路
6

【図2】


01011010
誤り検出用冗長ビット（原データ）
1. 入力暗号文
1011....
....1001
10110010
情報ビット（56ビット）
冗長ビット（8ビット）
9. 出力平文（誤った鍵データにより解読された場合）
1001....
....1011
01110010
情報ビット（56ビット）
冗長ビット（8ビット）
9. 出力平文（正しい鍵データにより解読された場合）
1100....
....0010
01011010
冗長ビットの内容が原データと一致する
情報ビット（56ビット）
冗長ビット（8ビット）

【図3】


13
有意性レベル設定回路
4
16
12
17
15
14
鍵データテーブル
鍵データテーブルアドレス発生回路
有意性判定回路
5
11
10
平文記憶回路
2
18
1
3
19
7
9
暗号文入力回路
暗号文記憶回路
暗号解読回路
平文出力回路
6
8

【考案の詳細な説明】

【０００１】

【産業上の利用分野】

この考案は、複数の鍵データを用いた暗号通信システムにおける暗号解読器に関するものである。

【０００２】

【従来の技術】

ディジタル通信の分野においては、情報源からの信号は、一般に“１”及び“０”の２値からなる数値列に変換され、この２値により、搬送信号を変調することによって無線または有線伝送路に送出され、目的地へ伝達される。情報源からの信号としては、例えば文字、音声や画像等があり、これらの情報源信号は伝送路上で容易に第三者の傍受が可能な状況にある。上記のように第三者が傍受可能な伝送路を使用して、情報を伝送する場合、秘匿性を有する情報源データについては情報源側で暗号化し、目的地の受信側でこれを暗号解読してもとの情報源からの信号を復元する、いわゆる暗号通信システムが構成される。

【０００３】

暗号通信システムとしては、様々な原理に基づくものが提案され、実用されているが、よく用いられる方式の一つに秘密鍵暗号方式と呼ばれるものがある。秘密鍵暗号方式では文字等の情報の順序を置き換える転置式、文字等の情報を他の文字等に置き換える換字式等が実用されている。これらの操作により、加工されて伝送路に送出される情報源からの情報は、どのような規則によって情報が加工されたかを知らない第三者には解読できず、その規則を知っている目的地の受信側でのみ、解読可能とするものである。従って、上記秘密鍵暗号方式では、送信側と受信側が知っている、暗号化するために使用する規則すなわち転置や換字の対応表を、第三者に知られないように保護することが重要になる。転置や換字の対応表は鍵と呼ばれることから、上記の方式は秘密鍵暗号方式と呼ばれる。ここで、鍵データは一定の期間、同一のものが使用されるが、通信の秘匿性を確保するためには同一の鍵データを長く使用するのは好ましくない。同一の鍵データを使用して長期間にわたって通信を続けた場合、傍受者にとって、同一鍵による通

信文の十分なサンプルを収集し、これを解析して暗号鍵を発見する、いわゆる既知平文攻撃等の十分な時間と機会を与えることになるからである。特に暗号のアルゴリズムが公開されている場合、鍵データの発見は一層容易になるため、鍵データは頻繁に交換できることが必要である。

【０００４】

さて、鍵データを交換する際には、当然送信側と受信側が同期して交換しなければ、受信側で暗号文を解読することができないことはいうまでもない。そこで、鍵データの配送はさまざまな方法でなされるが、例えば、暗号文を送受する通信路とは別の手段によって配送できれば、安全性が高い。暗号文の通信が有線による電気通信で行われる系においては、予め送信側から暗号鍵データを交換する日時と新しい暗号鍵データを物理的な手段で受信側に配送し、受信側でこれらにもとづいて暗号解読機の各パラメータをセットする場合を考えると、第三者はこれを傍受する手段を持たず、高い安全性が確保できる。

【０００５】

しかし、特に送信側と受信側の距離が著しく離れており、通信の伝送路以外の配送手段を持たない場合、即ち、鍵データを配送する物理的な手段を持たない場合は、鍵データの配送そのものも第三者の傍受可能な通信路によらぜるを得ないことになる。この場合、鍵データを配送する通信路自体が第三者の傍受が可能であり、鍵データを解読される危険があるため、鍵データの更新は行われず、鍵データ記憶回路に初期設定された鍵データが連続的に使用されることになる。従って、このような場合において安全に鍵データを交換する手段の必要性が生じる。

【０００６】

図４は、秘密鍵暗号方式における、鍵配送手段を具備した従来のデータ暗号装置の例であり、図において１は入力暗号文、２は暗号文入力回路、３は暗号文、５は鍵データ、６は暗号解読回路、７は平文、８は平文出力回路、９は出力平文、２０は鍵データ判別回路、２１は更新鍵データ、２２は鍵データ記憶回路である。

【０００７】

次に動作について説明する。入力暗号文１は暗号文入力回路２で受信され、暗

号文３として、暗号解読回路６へ入力される。一方、暗号解読回路６において暗号を解読するための鍵データ５は、鍵データ記憶回路２２から暗号解読回路６に供給される。暗号解読回路６は、鍵データ５を用いて、暗号文３を解読し、その結果を平文７として出力する。平文７は、平文出力回路８から出力平文９として出力される。ここで暗号文入力回路２は入力データを暗号解読回路で処理するためのバッファの機能を有する。例えば、入力暗号文１がシリアルデータ形式の場合、暗号文入力回路２はこれを暗号文解読回路６が同時に処理するビット数からなるパラレルデータに変換する。また、平文出力回路８では逆に、暗号文解読回路から出力されるパラレルデータを、再びシリアルデータに変換する機能を有する。

【０００８】

ここで、暗号文３は暗号解読回路４によって解読され、平文７が平文出力回路８を経て出力平文として出力されるが、平文７は同時に鍵データ判別回路２０へも供給される。鍵データ判別回路では、平文７に含まれる特定の情報を検出し、鍵データの配送であることを判別すると、検出された更新鍵データ２１を鍵データ記憶回路２２に供給する。鍵データ記憶回路の鍵データは、このようにして更新され、これ以降の暗号解読回路４への鍵データは、新しいデータが使用される。送信側では、上記鍵データの配送を行ったあと自らの暗号化鍵も更新して、暗号化を行うため、送信及び受信側で同期した鍵データの更新が可能になる。送信側が任意の時点で鍵データの変更を行う際に、鍵データを特定の方法で暗号文として暗号文の通信路から送信し、受信側ではこれを受信して、上記特定の方法で暗号化された鍵データであるかを判別し、鍵データの配送であることが検出された場合は、鍵データの更新を行い、これ以降の暗号解読は新しい鍵データによって行うことが可能となっている。

【０００９】

【考案が解決しようとする課題】

前記の実施例では、鍵データの配送を暗号文の通信路を経て行い、暗号文通信路以外に鍵データの配送を行うことができない通信系においても、暗号文通信路を経由して、任意に鍵データの配送を行うことによって、上記通信路を傍受する

第三者による暗号鍵データの解読は困難であるが、一方、何らかの原因により、送信側において一旦受信側で受信された更新鍵データを見失った場合、それを知りうる手段をもたず、これ以降の通信が不可能になるという課題があった。即ち、鍵データ記憶回路へ書き込まれる鍵データが誤りを含んでいる場合、あるいは一旦書き込まれた鍵データの一部のビットが、雑音またはソフトエラーにより、反転する等、誤りの生じる可能性がある。

【0010】

本考案は、鍵データの配送を通信の伝送路自体を使用せざるを得ない系において、第三者の解読が不可能なデータ暗号装置を得ることにある。

【0011】

前期した従来の課題に対処するために、送信側から受信側へ通信の伝送路を経由して配送することなく、送信側で使用する鍵データを任意に変更し、かつ受信側で鍵データが変更されたことを検知し、以降の復号を新しい鍵データを使用して行うことにより、以後の通信を可能とするものである。

【0012】

【課題を解決するための手段】

この考案に係るデータ暗号装置は、受信側であらかじめ複数の鍵データを収納したテーブルを保有し、送信側から暗号解読のために使用する鍵データを、受信側に送信することなく、受信側が鍵データ収納テーブルの内容を自動的に検索し、鍵データを送信側のものに合わせて復号することを可能としたものである。

【0013】

【作用】

この考案におけるデータ暗号装置は、送信側で使用する鍵データを任意に変更した場合にも、受信側が送信側の鍵データの変更を自動的に検知し、以降の通信を可能とするものである。

【0014】

【実施例】

実施例1.

図1は、この考案の一実施例を示すデータ暗号装置のブロック図であり、図に

おいて1は入力暗号文、2は暗号文入力回路、3は暗号文、4は鍵データテーブル、5は鍵データ、6は暗号解読回路、7は平文、8は平文出力回路、9は出力平文、10は平文記憶回路、11は記憶平文である。また、12は記憶平文11についてその有意性を判定する平文有意性判定回路、13は有意性の有無を判定するレベルを設定する有意性レベル設定回路、14は設定された有意性レベル、15は平文の有意性判定結果フラグ、16は鍵データテーブルアドレス発生回路、17は鍵データテーブルアドレスである。

【0015】

さて上記の実施例では、平文出力回路8の出力平文9は平文記憶回路10に一旦記憶され、平文記憶回路10の記憶平文11は平文有意性判定回路12へ入力される。平文有意性判定回路12では、有意性レベル設定回路13にあらかじめ設定された有意性レベル14を基準に記憶平文11の有意性を判定し、その結果を有意性判定結果フラグ15として出力する。鍵データテーブルアドレス発生回路16は、上記有意性判定結果フラグ15が有意性があることを示す場合には、既に設定されているアドレスを変更せず、一方有意性がないことを示す場合には、鍵データテーブルアドレス17を変更して鍵データテーブル4の新しいデータを促す。

【0016】

上記の実施例における具体的な動作を説明する。鍵データテーブル4にN種（NはN≧2なる整数）の鍵データが格納されているものとする。送信側の暗号化装置もまったく同一の鍵データテーブルを使用しており、送信側及び受信側とも現在そのうちn番目（nは1≦n≦Nなる整数）の鍵データを使用している状態にあるとする。この状態では、受信側は送信側で暗号化に使用された鍵データと全く同じ鍵データを使用して暗号解読するため、正しい平文出力が得られる。ある時点で、送信側が鍵データを変更した場合を考える。送信側で新たに選択した鍵データが鍵データテーブルの（n＋1）番目のものである場合、受信側でn番目の鍵データを使用して解読された結果として、正しい平文出力は得られない。この時、平文記憶回路10には誤った出力平文9が記憶され、平文有意性判定回路12ではその有意性を判定した結果として、有意性判定結果フラグ15を非有

意状態にセットする。鍵データテーブルアドレス設定回路１６では、有意性判定結果フラグが非有意状態の時、鍵データテーブルアドレス１７を１インクリメントする。この結果、鍵データテーブル４の発生する鍵データが更新される。

【００１７】

実施例２.

ここで、平文の有意性判定を行う方法は、各種のものが考えられる。例えば、単純な実施例を図２に示す。図において、暗号化される前の平文として５６ビットの情報ビットに８ビットの誤り検出用冗長ビットを付加し、６４ビットの平文を１ブロックとするブロック暗号を考える。暗号鍵は平文長と同じく６４ビットであり、送信側では６４ビットの暗号文を、６４ビットの鍵データによりあらかじめ定められたアルゴリズムに従って暗号化し、６４ビットの暗号文を生成する。一方受信側では、これを６４ビットの鍵データにより暗号解読して、６４ビットの平文を再生する。今、送信側で使用する暗号が変更された場合、受信側ではこれを知りえず、暗号化に使用された鍵データと異なった鍵データで解読するため、出力される平文データとして誤った平文データが得られる。従って、８ビットの誤り検出用冗長ビットに誤りを発生し、平文有意性判定回路１２では誤り検出用冗長ビットを監視することにより、鍵データの変更を知ることができる。ここで、有意性レベル設定回路１３では、許容誤りビット数を設定する。即ち、誤りを全く許容しない場合には０ビット、誤りを許容する場合にはその許容ビット数をあらかじめ設定しておく。

【００１８】

鍵データに誤りが検出されると、前記のように、有意性判定結果フラグ１５により鍵データテーブルアドレス発生回路１６は鍵データテーブルアドレス１７を１インクリメントする。鍵データテーブル４はインクリメントされた新しい鍵データを選択して暗号解読回路６に供給するため、これ以降の暗号解読は新しい鍵データを使用して行われることになる。

【００１９】

送信側で変更する鍵データは、必ずしも使用中の次の鍵データテーブルアドレスに限定されず、従って例えば５アドレス先の鍵データに変更した場合は、上記

のように1インクリメントした受信側ではこれ以降の入力暗号文を正しく解読することは出来ない。この場合、送信側において、同一の新しい暗号文を5回送信すれば、5回目の受信によりアドレスが合計5インクリメントされるため、正しい解読が可能になる。送信側において、鍵データを変更した場合には、その直後の送信時にインクリメントしたアドレス分重複して同一の暗号文を送信することにより、受信側の鍵データを正しく設定することが可能になる。

【0020】

実施例3.

この考案の別の実施例を図3に示す。図において、1～17は図1と同様であるが、18は暗号文記憶回路であり、暗号文入力回路1と暗号解読回路6の間に挿入され、暗号文記憶回路18において記憶された記憶暗号文19が暗号文解読回路6へ供給される。このようにすることによって、入力暗号文は次の暗号文が入力されるまで保持され、平文有意性判定回路12において、鍵データの変更が検知された場合、鍵データテーブルアドレス発生回路16によるインクリメント動作を反復することにより、ループを連続的に動作させ、暗号文記憶回路18に記憶された暗号文自体を解読することが可能になる。従ってこの場合、実施例1のように送信側で何回も同じ暗号文を送信することなく、解読及び新しい鍵データへの更新が可能になる。

【0021】

【考案の効果】

以上のように、この考案によれば暗号文の送受に使用する通信路以外に鍵データを配送する手段を持たないシステムにおいて、送信側から鍵データを受信側に配送することなく、鍵データの変更が可能となる。従って、暗号文通信路以外に鍵データの配送を行うことができない通信系においても、暗号文通信路を経由して、鍵データを配送する場合に考えられる傍受の危険性を回避し、しかも鍵データの配送中に鍵データに誤りを生じた場合にもたらされる通信の途絶を回避できる効果がある。